CLAIMS

1. A method of recovering target data provided in encrypted form to a party as part of a data set with which first and second trusted authorities are associated in a non-subvertible manner, the method comprising:

providing a first element to the party after the first trusted authority has verified that a specific individual is a professional accredited with it;

providing a second element to the party after both the second trusted authority has verified that a particular organisation is accredited with it, and said particular organisation has verified that said specific individual is engaged by it; and

the party using both said elements to recover the target data in clear;

at least one of the particular organisation and the first trusted authority ensuring that its verification is for said party as said specific individual before providing the corresponding element.

2. A method according to claim 1, wherein said data set comprises an encrypted first item decryptable using a first decryption key obtainable from the first trusted authority and an encrypted second item decryptable using a second decryption key obtainable from the second trusted authority, both items requiring decryption for the target data to be recovered in clear; the method comprising:

(a) providing the party, in a secure manner, with the first element from the first trusted authority only if the latter is satisfied that the party is a professional accredited with this authority, the first element being one of the first decryption key and the first item recovered with this key;

(b) providing said particular organisation, in a secure manner, with the second decryption key, or the second item decrypted with this key, from the second trusted authority only if the latter is satisfied that the particular organisation is accredited with this authority;

(c) providing the party with the second element from said particular organisation only if the organisation is satisfied that the party is engaged by the organisation with authority to access the target data, the second element being one of the second decryption key and the second item recovered with this key; and

(d) recovering the target data at the party by using the decrypted first and second items, decryption of the target data being effected at the party.

3. A method according to claim 2, wherein the particular organisation provides its output to said party in a secure manner.

4. A method according to claim 2, wherein:

the first item has been encrypted, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of the first trusted authority; the first decryption key being a key generated by the first trusted authority in dependence both on the first encryption key string and on private data related to said public data; and

the second item has been encrypted, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that identifies a specific organisation, and public data of the second trusted authority; the second decryption key being a key generated by the second trusted authority in dependence both on the second encryption key string and on private data related to said public data; the second decryption key, or the second item recovered with this key, only be provided to said particular organisation upon the second trusted authority being satisfied that said particular organisation is the specific organisation identified in the second encryption key string as well it as being an organisation accredited with the second trusted authority.

5. A method according to claim 4, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the second item being recovered using the second decryption key and then being subject to decryption using the first decryption key to recover the target data.

6. A method according to claim 4, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the second item being

recovered using the second decryption key to provide said nonce which is then combined with the identifier of said specific individual to form the first encryption key string, this key string thereafter being provided to the first trusted authority in order to enable the latter to provide the first decryption key for use at said party to decrypt the first item and thereby recover the target data.

7. A method according to claim 4, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the first and second items being independently recovered to provide the first and second data which are then used at said party to form said symmetric key, this key then being used to decrypt the target data.

8. A method according to claim 4, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the first and second items being independently recovered to provide the encrypted first symmetric key and the second symmetric key, and the second symmetric key then being used at said party to decrypt the encrypted first symmetric key after which the first symmetric key is used to decrypt the encrypted target data.

9. A method according to claim 4, wherein the party is provided with multiple different encrypted target datas in respective data sets, the first item of each data set being encrypted with a first encryption key string that comprises, in addition to identification of said specific individual, a random element; the party, in recovering each target data, obtaining from the first trusted authority, the corresponding first decryption key or the corresponding first item recovered using this key.

10. A method according to claim 4, wherein the party is provided with multiple different encrypted target datas in respective data sets, the first item of each data set being encrypted with the same first encryption key string; the party, after having obtained the corresponding

first decryption key from the first trusted authority in the course of recovering the target data of one data set, caching the first decryption key and re-using it from cache for recovering the target datas of subsequent data sets that have first items encrypted using the same first encryption key string as that for which the cached first decryption key was obtained.

11. A method according to claim 4, wherein the party is provided with multiple different encrypted target datas in respective data sets, the second item of each data set being encrypted with a second encryption key string that comprises, in addition to identification of said specific organisation, a random element; the requesting organisation obtaining from the second trusted authority, for each different second encryption key string used, the corresponding second decryption key or the corresponding second item recovered using this key.

12. A method according to claim 4, wherein the party is provided with multiple different encrypted target datas in respective data sets, the second item of each data set being encrypted with the same second encryption key string; the requesting organisation after having obtained the corresponding second decryption key from the second trusted authority in respect of one data set, caching the second decryption key and re-using it from cache for subsequent data sets that have second items encrypted using the same second encryption key string as that for which the cached second decryption key was obtained, the requesting organisation decrypting the second item itself and passing the recovered second item to said party.

13. A method according to claim 1, wherein said data set comprises an encrypted first item decryptable using a first decryption key obtainable from the first trusted authority and an encrypted second item decryptable using a second decryption key obtainable from the second trusted authority, both items requiring decryption for the target data to be recovered in clear and the data set identifying said specific individual; the method comprising:

(a) providing the party with the first element from the first trusted authority only if the latter is satisfied that said specific individual, as identified in the data set, is a

professional accredited with this authority, the first element being one of the first decryption key and the first item recovered with this key;

(b) providing said particular organisation, in a secure manner, with the second decryption key, or the second item decrypted with this key, from the second trusted authority only if the latter is satisfied that the organisation is accredited with this authority;

(c) providing the party with the second element, from said particular organisation only if the latter is satisfied that said specific individual is engaged by the organisation with authority to access the target data, the second element being one of the second decryption key and the second item recovered with this key; and

(d) recovering the target data at the party by using the decrypted first and second items, decryption of the target data being effected at the party;

at least one of the first trusted authority and said particular organisation providing its associated element to said party in a secure manner and only after being satisfied that the party is the said specific individual identified in the data set.

14. A method according to claim 13, wherein:

the first item has been encrypted, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of the first trusted authority; the first decryption key being a key generated by the first trusted authority in dependence both on the first encryption key string and on private data related to said public data; and

the second item has been encrypted, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that identifies a specific organisation, and public data of the second trusted authority; the second decryption key being a key generated by the second trusted authority in dependence both on the second encryption key string and on private data related to said public data; the second decryption key, or the second item recovered with this key, only be provided to said particular organisation upon the second trusted authority being satisfied that said particular organisation is the specific organisation identified in the second

encryption key string as well it as being an organisation accredited with the second trusted authority.

15. A method according to claim 14, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the second item being recovered using the second decryption key and then being subject to decryption using the first decryption key to recover the target data.

16. A method according to claim 14, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the second item being recovered using the second decryption key to provide said nonce which is then combined with the identifier of said specific individual to form the first encryption key string, this key string thereafter being provided to the first trusted authority in order to enable the latter to provide the first decryption key for use at said party to decrypt the first item and thereby recover the target data.

17. A method according to claim 14, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the first and second items being independently recovered to provide the first and second data which are then used at said party to form said symmetric key, this key then being used to decrypt the target data.

18. A method according to claim 14, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the first and second items being independently recovered to provide the encrypted first symmetric key and the second symmetric key, and the second symmetric key then being used at said party to decrypt the encrypted first symmetric key after which the first symmetric key is used to decrypt the encrypted target data.

19. A method according to claim 14, wherein the party is provided with multiple different encrypted target datas in respective data sets, the first item of each data set being encrypted with a first encryption key string that comprises, in addition to identification of said specific individual, a random element; the party, in recovering each target data, obtaining from the first trusted authority, the corresponding first decryption key or the corresponding first item recovered using this key.

20. A method according to claim 14, wherein the party is provided with multiple different encrypted target datas in respective data sets, the first item of each data set being encrypted with the same first encryption key string; the party, after having obtained the corresponding first decryption key from the first trusted authority in the course of recovering the target data of one data set, caching the first decryption key and re-using it from cache for recovering the target datas of subsequent data sets that have first items encrypted using the same first encryption key string as that for which the cached first decryption key was obtained.

21. A method according to claim 14, wherein the party is provided with multiple different encrypted target datas in respective data sets, the second item of each data set being encrypted with a second encryption key string that comprises, in addition to identification of said specific organisation, a random element; the requesting organisation obtaining from the second trusted authority, for each different second encryption key string used, the corresponding second decryption key or the corresponding second item recovered using this key.

22. A method according to claim 14, wherein the party is provided with multiple different encrypted target datas in respective data sets, the second item of each data set being encrypted with the same second encryption key string; the requesting organisation after having obtained the corresponding second decryption key from the second trusted authority in respect of one data set, caching the second decryption key and re-using it from cache for subsequent data sets that have second items encrypted using the same second encryption key string as that for which the cached second decryption key was obtained, the requesting

organisation decrypting the second item itself and passing the recovered second item to said party.

23. A secure data-provision method comprising providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the target data being provided in encrypted form as part of a data set that comprises:

a first item encrypted, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

a second item encrypted according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations;

recovery of the target data in clear requiring decryption of both the first and second items.

24. A method according to claim 23, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

25. A method according to claim 23, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

26. A method according to claim 23, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

27. A method according to claim 23, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second

item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

28. A secure data-provision method comprising providing target data from a data provider to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the target data being provided in encrypted form as part of a data set that comprises:

a first item encrypted using both a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations; and

a second item encrypted using both a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations;

recovery of the target data in clear requiring decryption of both the first and second items.

29. A system for recovering target data provided in encrypted form to a party as part of a data set with which first and second trusted authorities are associated in a non-subvertible manner, the system comprising:

a first computing entity, associated with the first trusted authority, for providing a first element to the party after verifying that a specific individual is a professional accredited with it;

a second computing entity associated with the second trusted authority;

a third computing entity, associated with a particular organisation, for providing a second element to the party after the second computing entity has verified that said particular organisation is accredited with it, and the third computing entity has verified that said specific individual is engaged by it; and

a fourth computing entity, associated with said party, for decrypting the target data using the first and second elements;

at least one of the first and third computing entities being arranged to ensure that its verification is for said party as said specific individual before providing the corresponding element to the party.

30. A system according to claim 29, wherein:

said data set comprises an encrypted first item decryptable using a first decryption key obtainable from the first trusted authority and an encrypted second item decryptable using a second decryption key obtainable from the second trusted authority, both items requiring decryption for the target data to be recovered in clear;

the first computing entity is arranged to provide said party, in a secure manner, with the first element only if it is satisfied that the party is a professional accredited with the first trusted authority, the first element being one of the first decryption key and the first item recovered with this key;

the second computing entity is arranged to provide said particular organisation, in a secure manner, with the second decryption key, or the second item decrypted with this key, only if it is satisfied that the particular organisation is accredited with the second trusted authority;

the third computing entity is arranged to provide said party with the second element only if it is satisfied that the party is engaged by said particular organisation with authority to access the target data, the second element being one of the second decryption key and the second item recovered with this key; and

the fourth computing entity is arranged to recover the target data by using the decrypted first and second items.

31. A system according to claim 30, wherein the third computing entity is arranged to provide its output to said party in a secure manner.

32. A system according to claim 30, wherein:

the first item has been encrypted, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of the first trusted authority; the first computing entity being arranged to generate the first decryption key in dependence both on the first encryption key string and on private data related to said public data; and

the second item has been encrypted, according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies a

specific organisation, and public data of the second trusted authority; the second computing entity being arranged to generate the second decryption key in dependence both on the second encryption key string and private data related to said public data, and the second computing entity being further arranged to provide the second decryption key, or the second item recovered using this key, to said particular organisation upon being satisfied that said particular organisation is the specific organisation identified in the second encryption key as well it as being an organisation accredited with the second trusted authority.

33. A system according to claim 32, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the fourth computing entity being arranged to:

recover the second item, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity, and

subject the second item to decryption, using the first decryption key obtained from the first computing entity, to recover the target data.

34. A system according to claim 32, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the fourth computing entity being arranged to:

recover the second item, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity,

combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string,

provide the first encryption key string to the first computing entity to obtain the first decryption key, and

use the first decryption key obtained from the first computing entity to decrypt the first item and thereby recover the target data.

35. A system according to claim 32, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the fourth computing entity being arranged to:

recover the first data, if not provided to it in decrypted form by the first computing entity, by using the first decryption key obtained from the first computing entity,

recover the second data, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity,

use the first data and the second data to form said symmetric key, and

use the symmetric key to decrypt the target data.

36. A system according to claim 32, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the fourth computing entity being arranged to:

recover the first item, if not provided to it in decrypted form by the first computing entity, by using the first decryption key obtained from the first computing entity,

recover the second item, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity,

use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and

use the first symmetric key to decrypt the encrypted target data.

37. A system according to claim 29, wherein:

said data set comprises an encrypted first item decryptable using a first decryption key obtainable from the first trusted authority and an encrypted second item decryptable using a second decryption key obtainable from the second trusted authority, both items requiring decryption for the target data to be recovered in clear and the data set identifying said specific individual;

the first computing entity is arranged to provide said party with the first element only if it is satisfied that said specific individual, as identified in the data set, is a

professional accredited with the first trusted authority, the first element being one of the first decryption key and the first item recovered with this key;

the second computing entity is arranged to provide said particular organisation, in a secure manner, with the second decryption key, or the second item decrypted with this key, only if it is satisfied that the organisation is accredited with the second trusted authority;

the third computing entity is arranged to provide the party with the second element only if it is satisfied that said specific individual is engaged by the organisation with authority to access the target data, the second element being one of the second decryption key and the second item recovered with this key; and

the fourth computing entity is arranged to recovering the target data by using the decrypted first and second items;

at least one of the first and third computing entities being arranged to provide the corresponding element to said party in a secure manner and only after being satisfied that the party is the said specific individual identified in the data set.

38. A system according to claim 37, wherein:

the first item has been encrypted, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of the first trusted authority; the first computing entity being arranged to generate the first decryption key in dependence both on the first encryption key string and on private data related to said public data; and

the second item has been encrypted, according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies a specific organisation, and public data of the second trusted authority; the second computing entity being arranged to generate the second decryption key in dependence both on the second encryption key string and private data related to said public data, and the second computing entity being further arranged to provide the second decryption key, or the second item recovered using this key, to said particular organisation upon being satisfied that said particular organisation is the specific

organisation identified in the second encryption key as well it as being an organisation accredited with the second trusted authority.

39. A system according to claim 38, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the fourth computing entity being arranged to:

recover the second item, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity, and

subject the second item to decryption, using the first decryption key obtained from the first computing entity, to recover the target data.

40. A system according to claim 38, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the fourth computing entity being arranged to:

recover the second item, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity,

combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string,

provide the first encryption key string to the first computing entity to obtain the first decryption key, and

use the first decryption key obtained from the first computing entity to decrypt the first item and thereby recover the target data.

41. A system according to claim 38, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the fourth computing entity being arranged to:

recover the first data, if not provided to it in decrypted form by the first computing entity, by using the first decryption key obtained from the first computing entity,

recover the second data, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity,

use the first data and the second data to form said symmetric key, and

use the symmetric key to decrypt the target data.

42. A system according to claim 38, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the fourth computing entity being arranged to:

recover the first item, if not provided to it in decrypted form by the first computing entity, by using the first decryption key obtained from the first computing entity,

recover the second item, if not provided to it in decrypted form by the third computing entity, by using the second decryption key obtained from the third computing entity,

use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and

use the first symmetric key to decrypt the encrypted target data.

43. Apparatus for the secure provision of target data to a party purporting to be a specific, professionally-accredited, individual engaged by a specific accredited organisation, the apparatus comprising an encryption subsystem for generating a data set including the target data in encrypted form, the encryption subsystem comprising:

first encryption means for encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, based on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations;

second encryption means for encrypting a second item, according to an IBE scheme, based on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations; and

means for forming the data set using at least the encrypted first and second items;

the recovery of the target data in clear requiring decryption of both the first and second items.

44. Apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises the encrypted first item.

45. Apparatus according to claim 43, wherein the first item comprises the target data, and the second item comprises a nonce; the first encryption key string comprising, in combination, an identifier of said specific individual and said nonce.

46. Apparatus according to claim 43, wherein the first item comprises first data, and the second item comprises second data; the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data.

47. Apparatus according to claim 43, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key.

48. A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data, the first item being encrypted in dependence on encryption parameters comprising a first encryption key string that identifies a specific individual and first public data, and the second item being encrypted in dependence on a second encryption key string that identifies a specific organisation and second public data; the entity comprising:

first means for requesting either a first decryption key corresponding to the first encryption key string, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string to the first trusted authority when making its

request and being further arranged to authenticate the entity with the first trusted authority and to receive the first decryption key, or the first item, securely from the first trusted authority;

second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organisation accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organisation when making its request and being further arranged to authenticate the entity with the organisation and receive the second decryption key, or the second item, from the organisation;

third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organisation, to recover the target data.

49. A computing entity according to claim 48, wherein the second means is arranged to receive the second decryption key, or the second item, securely from the organisation.

50. A computing entity according to claim 48, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to:

recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, and

subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data.

51. A computing entity according to claim 48, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to:

recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation,

combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority, and

use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data.

52. A computing entity according to claim 48, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to

recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority,

recover the second data, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation,

use the first data and the second data to form said symmetric key, and

use the symmetric key to decrypt the target data.

53. A computing entity according to claim 48, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to:

recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority,

recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation,

use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and

use the first symmetric key to decrypt the encrypted target data.

54. A computing entity for recovering target data provided in encrypted form as part of an data set that comprises first and second encrypted items both of which must be decrypted to recover the target data; the first item being encrypted in dependence on a first encryption key string that identifies a specific individual, and first public data; and the second item being encrypted in dependence on a second encryption key that identifies a specific organisation and said specific individual, and second public data; the entity comprising:

- first means for requesting either a first decryption key corresponding to the first encryption key, or the first item in decrypted form, from a first trusted authority which is competent in respect of the accreditation of professionals and holds first private data related to the first public data, the first means being arranged to provide the first encryption key string, or the first item, to the first trusted authority when making its request;
- second means for requesting either a second decryption key corresponding to the second encryption key string, or the second item in decrypted form, from an organisation accredited by a second trusted authority which holds second private data related to the second public data, the second means being arranged to provide the second encryption key string to the organisation when making its request; and
- third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organisation, to recover the target data;

at least one of the first means and the second means being arranged to authenticate the entity to the first trusted authority or said organisation as the case may be and to receive input therefrom in a secure manner.

55. A computing entity according to claim 54, wherein the first item comprises the target data, and the second item comprises the encrypted first item; the third means being arranged to:

recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation, and subject the second item to decryption, using the first decryption key obtained from the first trusted authority, to recover the target data.

56. A computing entity according to claim 54, wherein the first item comprises the target data, the second item comprises a nonce, and the first encryption key string comprises, in combination, an identifier of said specific individual and said nonce; the third means being arranged to:

recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation,

combine the nonce that formed the second item with the identifier of said specific individual in order to form the first encryption key string to be provided by the first means to the first trusted authority, and

use the first decryption key obtained from the first trusted authority to decrypt the first item and thereby recover the target data.

57. A computing entity according to claim 54, wherein the first item comprises first data and the second item comprises second data, the data set further comprising said target data encrypted using a symmetric key that can be formed by using both said first and second data; the third means being arranged to

recover the first data, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority,

recover the second data, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation,

use the first data and the second data to form said symmetric key, and

use the symmetric key to decrypt the target data.

58. A computing entity according to claim 54, wherein the data set comprises, in addition to said first and second items, said target data encrypted using a first symmetric key, the second item comprising a second symmetric key, and the first item comprising the first symmetric key encrypted using the second symmetric key; the third means being arranged to:

recover the first item, if not provided to the first means by the first trusted authority, by using the first decryption key obtained from the first trusted authority,

recover the second item, if not provided to the second means in decrypted form by the organisation, by using the second decryption key obtained from the organisation,

use the second symmetric key that formed the second item to decrypt the encrypted first symmetric key that formed the first item, and

use the first symmetric key to decrypt the encrypted target data.